UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

R. ANDRE KLEIN, individually and on behalf of all others similarly situated, Plaintiff, v. LASTPASS US LP, and GOTO TECHNOLOGIES USA, INC., Defendants.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff R. Andre Klein ("Plaintiff"), individually on behalf of himself and all other persons similarly situated, asserts the following against Defendants LastPass US LP ("LastPass" or the "Company") and GoTo Technologies USA, Inc. ("GoTo") (collectively, "Defendants"), based upon his personal knowledge with respect to himself and his own acts, and upon information and belief, and the investigation of counsel, as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This action arises out of Defendants' failure to protect its customers' private and personal information during two related data breaches that began in August 2022 ("LastPass Data Breaches" or "Data Breaches").

2. Defendants' failure to protect its customers' data is particularly egregious in light of their business of providing cloud security technology. Defendant LastPass is a software company that provides its registered users with tools to store and protect their passwords, a security dashboard, dark web monitoring, and other services that are purchased by Defendants' customers to protect their personal information. Indeed, the sole reason that Plaintiff and the Class Members

used LastPass and provided Defendants with their personally identifiable information ("PII") was to have their passwords and PII protected and minimize the risk of data breaches.

3. But Defendants failed to provide the services that they promised and that Plaintiff and the Class Members purchased. Plaintiff and the Class Members provided their PII to Defendants in order to improve the security of their personal data. However, rather than protect that data, Defendants implemented lax data privacy and security protocols. Thus, not only did data thieves gain access to a cloud-based storage service used by Defendants, steal access and decryption keys, and then copy the PII of Plaintiff and the Class Members, but when Defendants learned about the first Data Breach in August 2022, they failed to timely or effectively remediate the breach. This allowed the data thieves to gain further unauthorized access using the information it initially compromised.

4. Even then, Defendants waited months to be fully transparent with Plaintiff and the Class Members. It was not until November 30, 2022, that Defendants provided notice that the Data Breaches resulted in the exfiltration of PII and until December 22, 2022—four months after the initial Data Breach—that Defendants finally revealed the full extent of the Data Breaches.

5. Information compromised in the Data Breaches includes first and last names, user names, company names, billing addresses, email addresses, telephone numbers, IP addresses that indicate the locations from which Plaintiff and Class Members were accessing websites, lists of the websites from which Plaintiff and Class Members accessed LastPass, and encrypted customer vaults. The customer vaults obtained by the data thieves further contain photographs, email, websites visited, passwords, notes, addresses, payment cards, and linked bank accounts.

6. The information not protected by LastPass in the customer vaults—namely, the IP addresses and lists of websites visited by users—can be used by bad actors to create both complete

movement profiles of a user's location on a daily basis, and in-depth knowledge of sensitive information about users–such as political leanings or sexual preferences.

7. LastPass has long been on notice that it is a target of data thieves and that it has lax security protocols—indeed, it has a history of data breach and security issues. Since 2011, LastPass has been exposed a number of times for suffering security incidents and failing to properly safeguard customer information. Despite being on notice of the threat, Defendants failed to both maintain and safeguard the PII of Plaintiff and Class Members in a manner consistent with the security representations presented to consumers in both their data privacy and security protocols and Terms and Services.

8. The Data Breaches made clear that Plaintiff and Class Members did not receive what they paid for as customers of LastPass. Moreover, as a result of the Data Breaches, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a diminution in the value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendants, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. Plaintiff and Class Members already have incurred, and will continue to incur, out-of-pocket costs for and have and will continue to spend substantial amounts of time taking protective measures to deter and detect identity theft as a result of the LastPass Data Breach.

9. Plaintiff brings this class action lawsuit on behalf of himself and all those similarly situated to address Defendants' failure to provide Class Members with the service they contracted for—protection of their PII. Plaintiff also brings this action to address Defendants' failure to provide timely and adequate notice to Plaintiff and the Class Members of the Data Breaches.

10. Accordingly, Plaintiff brings this action, on behalf of himself and all others similarly situated, against Defendants seeking redress for their unlawful conduct. Plaintiff asserts claims for (1) negligence, (2) negligent misrepresentation, (3) breach of express contract, (4) breach of implied contract, and (5) unjust enrichment.

II. PARTIES

A. Plaintiff

11. Plaintiff R. Andre Klein ("Plaintiff") is a natural person and citizen of the State of New York and resident of Willsboro, New York.

B. Defendants

12. Defendant LastPass US LP ("LastPass" or "the Company") is a limited partnership organized under the laws of Delaware with its principal place of business in Boston, Massachusetts.

13. Defendant GoTo Technologies USA, Inc. ("GoTo"), f/k/a LogMeIn, is a Delaware corporation with its principal place of business in Boston, Massachusetts. GoTo is a LastPass affiliate authorized to provide and support LastPass services. Formerly known as LogMeIn, GoTo is a provider of software and cloud-based remote work tools. LogMeIn acquired LastPass in 2015 and later rebranded as GoTo in 2022.

III. JURISDICTION AND VENUE

14. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, including the Plaintiff, are citizens of states different than that of Defendant.

15. This Court has personal jurisdiction over Defendants LastPass and GoTo because (1) both Defendants maintain their principal place of business in Massachusetts and (2) both Defendants conduct substantial business in and throughout Massachusetts.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendants are authorized to conduct business within this District, are headquartered in this District, have intentionally availed itself of the laws in this District, and conduct substantial business, including acts underlying the allegations of this complaint, in this District.

IV. FACTUAL ALLEGATIONS

A. LastPass Misrepresents Itself To Users Seeking Digital Security As 'Leading the Way' On Data Privacy And Security

17. Defendant LastPass is a software company that describes itself as "leading the way in password security and identity management for personal and business digital safety."[1] First founded in 2008, LastPass provides software tools to registered users that are meant to centralize the storage and protection of passwords for users.

18. A study published in May 2022 by the International Data Corporation projects that the amount of new data created, captured, replicated, and consumed is expected to double in size by 2026.[2] With an increase in data creation comes a heightened risk of data breaches and bad actors gaining access to personal information. One result of data breaches, identity theft, poses a serious threat to consumers engaging in online transactions and across a host of digital platforms.

[1] About LastPass, https://www.lastpass.com/company/about-us (last visited Jan. 18, 2023).
[2] *See* John Rydning, Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth, IDC, *available at* https://www.idc.com/getdoc.jsp?containerId=US49018922 (last visited Jan. 18, 2023).

Both state and federal laws and regulations impose standards of reasonable security measures for businesses so consumers can, in turn, feel safe sharing their PII in the marketplace.

19. For example, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair practice of failing to use reasonable data privacy and security measures to protect data. To help businesses come into compliance with the FTC Act, the FTC has promulgated guides aimed at educating businesses about the importance of security protocols.[3] Under the FTC Act, Defendants have duties to implement reasonable security measures to protect user data.

20. In addition, Massachusetts regulations require an entity that owns or licenses personal information about a resident of Massachusetts to meet minimum standards in safeguarding that personal information. Under 201 Mass. Code Regs § 17, these entities are required, in part, to include both (1) "[r]easonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage or containers," and (2) "[r]egular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks."

[3] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf/ (last visited Jan. 18, 2023). *See also* Federal Trade Commission, Start With Security: A Guide For Business, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 18, 2023; Federal Trade Commission, Start With Security: Lessons Learned From FTC Cases (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 18, 2023).

21. In the context of and with knowledge of the increasing threat of data breaches to consumers, LastPass has used the uptick in cybersecurity risk to tout its business model on the company website "About Us" page:

> Data breaches are on the rise, with more than 80% of breaches caused by weak, reused, or stolen passwords. Doing nothing could mean losing everything. That's why password security has never been more critical for individuals and businesses.
>
> As a pioneer in cloud security technology, LastPass provides award-winning password and identity management solutions that are convenient, effortless, and easy to manage. LastPass values users' privacy and security, so your sensitive information is always hidden – even from us.

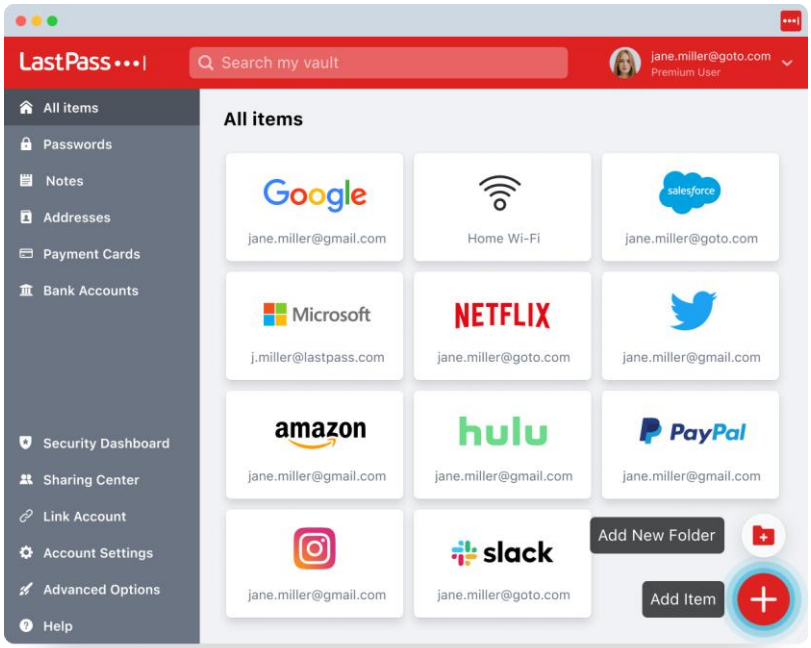
22. LastPass users, therefore, pay Defendants to provide data privacy and security services that keep their passwords and PII centralized and secure. The consumer demand for this data privacy and security service is evidenced by LastPass's published user statistics, as the Company claims to have over 33 million individuals and 100,000 businesses as registered users.[4]

23. LastPass offers a variety of tools that purport to help registered users save and access their passwords. Once a user has a LastPass account, they can use that account to log in to both the LastPass password browser extension and LastPass password manager app for mobile devices to access and save passwords.

24. LastPass users are prompted to create a "master password" through which they can then access their "LastPass password manager vault." LastPass then records the websites for which its customers maintain accounts, as well as the login information for those sites to the vault. LastPass also stores the IP addresses users visit, showing the geolocation from which a user connects to the internet.

[4] *See* About LastPass, https://www.lastpass.com/company/about-us (last visited Jan. 18, 2023).

25. An image of the LastPass password manager vault on the LastPass website indicates that a user's vault dashboard can include a user's name, photograph, email, websites visited, passwords, notes, addresses, payment cards, and linked bank accounts.



5

26. LastPass states that it is designed to keep sensitive data safe using a "local-only, zero knowledge security model."[6] LastPass describes the product architecture as follows:

> The LastPass service features a vault, in which sensitive user data is stored and, based on utilization of a 'zero-knowledge' framework, accessed only by entering the user's master password, which is not maintained in unencrypted form by LastPass -- LastPass does not store and cannot access this password. User data input via the LastPass web or mobile application is encrypted with the user's unique key on their device and the AES-256 encrypted data is synced to LastPass for secure

[5] *See* How to Use LastPass Manager, https://www.lastpass.com/how-lastpass-works (last visited Jan. 18, 2023).
[6] *See* Our Zero-Knowledge Security Model, https://www.lastpass.com/security/zero-knowledge-security (last visited Jan. 18, 2023).

storage. The user can access and decrypt their data on demand with their master password – which occurs entirely at the user and device-level.[7]

27. LastPass promotes its services to three different profiles of users: (1) business users, (2) personal-use users, and (3) partner-purchaser users. Under the Terms of Service for Personal Use, LastPass provides the following representations:[8]:

> "4.2 Your Privacy and Security
>
> 4.2.1. Information Security and Certifications
>
> **We have implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure**. We also maintain a compliance program that includes independent third-party audits and certifications. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center) to review Service-specific information about our technical and organizational security measures (located in the Technical and Organizational Measures or "TOMs" documentation), including, but not limited to, encryption use and standards, retention periods, and other helpful information.
>
> 4.2.2. Data Privacy
>
> **We maintain a global data privacy program, designed to safeguard and responsibly handle your Content and any associated personal data we may collect and/or process on your behalf**. You understand that when using the Services or interacting with our websites your personal data may be processed via equipment and resources located in the United States and other locations throughout the world. You can visit our Trust & Privacy Center (https://www.lastpass.com/trust-center/privacy) to review LastPass' comprehensive privacy program, third-party frameworks, privacy policies, and applicable data processing locations and Sub-Processor Disclosures, as well as the TOMs."[9]
>
> 8.7. Security Emergencies

---

[7] *See* Technical and Organizational Measures For LastPass, https://www.lastpass.com/-/media/175854c49fcb489baeaa87e78579e28f.pdf (last visited Jan. 18, 2023).

[8] *See* LastPass Terms of Service for Personal Use (2022), https://www.lastpass.com/legal-center/terms-of-service/personal (last visited Jan. 18, 2023).

[9] This same section can be found at "4.2 Your Privacy and Security" in the LastPass Terms of Service for Business Customers, https://www.lastpass.com/legal-center/terms-of-service/business, and "3.2 Your Privacy and Security" in the Terms of Service for Partner Sales, https://www.lastpass.com/legal-center/partner-sales-terms.

> If we reasonably determine that the security of the Services or infrastructure may be compromised due to hacking attempts, denial of service attacks, or other malicious activities, we may temporarily suspend the Services. If we do so, we will, to the extent practicable, provide you notice, and take actions designed to promptly resolve any security issues and restore the Services.[10]

28. Further describing LastPass's "foundation of security," the Company also states on its website, relative to "transparent incident response," the following: "Our team reacts swiftly to reports of bugs or vulnerabilities and communicates transparently with our community."[11]

B. LastPass's History of Security Issues

29. LastPass has been exposed a number of times in the past for failing to safeguard customer information.

30. On May 3, 2011, LastPass suffered a security incident. LastPass was unable to state for certain that customer information was not breached, requiring some users to change their master passwords as a precaution.[12]

31. On June 15, 2015, LastPass posted blog post stating that LastPass had suffered a data breach.[13] The LastPass investigation revealed that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised.

---

[10] This same section can be found at "9.5 Security Emergencies" in the LastPass Terms of Service for Business Customers, https://www.lastpass.com/legal-center/terms-of-service/business, and "8.5 Security Emergencies" in the Terms of Service for Partner Sales, https://www.lastpass.com/legal-center/partner-sales-terms.

[11] *See* Our Zero-Knowledge Security Model, https://www.lastpass.com/security/zero-knowledge-security (last visited Jan. 18, 2023).

[12] *See* JR Raphael, *LastPass CEO Explains Possible Hack*, PCWorld (May 5, 2011), https://www.pcworld.com/article/491164/lastpass_ceo_exclusive_interview.html.

[13] *See* Joe Siegrist, LastPass Hacked – Identified Early & Resolved, Update as of June 15, 2015, https://blog.lastpass.com/2015/06/lastpass-security-notice/ (last visited Jan. 18, 2023).

32. In July 2016, a vulnerability was discovered by independent online security firm Detectify. Detectify published a blog post on the vulnerability, describing it as a bug in the autofill function that allowed for the extraction of passwords.[14]

33. In March 2017, a vulnerability was discovered in the LastPass browser extension for Chrome that applied to all LastPass clients.[15]

34. In August 2019, a vulnerability in the LastPass browser extension for Chrome and Opera browsers allowed malicious websites to steal credentials for the last account the user logged into.

35. In 2020, a vulnerability in the LastPass browser extension where the extension would store a user's master password in a local file when the "Remember password" option was activated.[16]

36. In 2021, it was discovered that the LastPass Android app contained seven third-party trackers that sent data to third-party companies and recorded user behavior.[17]

37. In December 2021, users reported that their LastPass master passwords appeared to be compromised. LastPass responded to the news, noting that they had been investigating reports of users receiving e-mails alerting them to block login attempts.[18]

---

[14] *See* Mathias Karlsson, *How I made LastPass give me all your passwords*, Detectify (Jul. 27, 2016), https://labs.detectify.com/2016/07/27/how-i-made-lastpass-give-me-all-your-passwords/.
[15] Travis Ormandy (@taviso), Twitter (Mar. 25, 2017), https://twitter.com/taviso/status/845717082717114368.
[16] *See* Oleg Afonin, *Breaking LastPass: Instant Unlock of the Password Vault* (Apr. 6, 2020), https://blog.elcomsoft.com/2020/04/breaking-lastpass-instant-unlock-of-the-password-vault/
[17] *See* Jon Porter, *Security researcher recommends against LastPass after detailing 7 trackers*, The Verge (Feb. 26, 2021), https://www.theverge.com/2021/2/26/22302709/lastpass-android-app-trackers-security-research-privacy.
[18] *See* Emma Roth, LastPass says no passwords were compromised following breach scare, The Verge (Dec. 29, 2021), https://www.theverge.com/2021/12/28/22857485/lastpass-compromised-breach-scare

C. The 2022 LastPass Data Breaches

1. LastPass August 2022 Breach and Statement

38. On August 25, 2022, LastPass first posted the following notice informing LastPass users of the August 2022 Data Breach, in a notice signed by LastPass CEO Karim Toubba ("Toubba"):

> To All LastPass Customers,
>
> I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.
>
> Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, **we have seen no evidence that this incident involved any access to customer data or encrypted password vaults**.
>
> We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally.
>
> In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. **While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity**.
>
> Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.
>
> Thank you for your patience, understanding and support.
>
> Karim Toubba
>
> CEO LastPass

39. In a supplemental "FAQs" portion of the post, Toubba stated the following relative to the data thieves' access to user data and personal information:

> **Has any data within my vault or my users' vaults been compromised?**
>
> No. This incident occurred in our development environment. Our investigation has shown no evidence of any unauthorized access to encrypted vault data. Our zero knowledge model ensures that only the customer has access to decrypt vault data.
>
> **Has any of my personal information or the personal information of my users been compromised?**
>
> No. Our investigation has shown no evidence of any unauthorized access to customer data in our production environment."
>
> Both of these statements by the LastPass CEO were false.

40. As to whether LastPass users should act to mitigate future risk in light of the Data Breach, Toubba further stated in the post, "***At this time, we don't recommend any action on behalf of our users or administrators***."

2. LastPass September Statement

41. On September 15, 2022, LastPass published an update ("September Statement") regarding the August 2022 Data Breach.[19]

42. In the September Statement, Toubba described the Company's investigation into the August 2022 Data Breach as "completed."

43. According to the September Statement, the investigation revealed that the August 2022 Data Breach spanned the total of four consecutive days before it was intercepted and ceased by LastPass.

44. Toubba also reiterated in the September Statement, that, "[w]e can also confirm that there is no evidence that this incident involved any access to customer data or encrypted password vaults." He also explained that "[a]lthough the threat actor was able to access the

[19] *See* Karim Toubba, Notice of Recent Security Incident, Update as of Thursday September 15, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last visited Jan. 18, 2023).

Development environment, our system design and controls prevented the threat actor from accessing any customer data or encrypted password vaults."

3. LastPass November Statement: Further Extent of Data Breaches Revealed

45. On November 30, 2022, LastPass published another update ("November Statement"), now regarding the second 2022 Data Breach ("Second 2022 Data Breach").[20]

46. In the November Statement, Toubba revealed that the Company's third-party cloud storage service—shared by both LastPass and GoTo—was breached by an unauthorized party. Using information obtained in the August 2022 Breach, this unauthorized party was able to obtain customers' PII.

47. Toubba explained that LastPass was "working diligently to understand the scope of the incident and identify what specific information has been accessed."

4. LastPass December Statement: Truth of the Second 2022 Data Breach Revealed

48. On December 22, 2022, LastPass published another post ("December Statement") on the cyber breach—finally acknowledging that core customer data was compromised as a result of both the August 2022 Breach and Second 2022 Data Breach.[21]

49. On December 22, 2022, Plaintiff received an email from LastPass prompting him to read the Company's update as to the Data Breaches.

---

[20] *See* Karim Toubba, Notice of Recent Security Incident, Update as of Wednesday November 30, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last visited Jan. 18, 2023).

[21] *See* Karim Toubba, Notice of Recent Security Incident, Update as of Thursday December 22, 2022, https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last visited Jan. 18, 2023).

50. In the December Statement, Toubba stated that "To date, we have determined that once the cloud storage access key and dual storage container decryption keys were obtained, the threat actor copied information from backup that contained basic customer account information and related metadata including company names, end-user names, billing addresses, email addresses, telephone numbers, and the IP addresses from which customers were accessing the LastPass service."

51. Toubba explained that the data thieves were also able to steal copies of backup customer vault data containing unencrypted data. This unencrypted data included website URLs.

52. In the December Statement, Toubba also explained LastPass's "best practices" as including the update in 2018 requiring new users to create a twelve-character-minimum master password.[22] After further outlining the post-2018 default settings, the LastPass CEO outlined the Company's advice to users following the Data Breach:

> **If you use the default settings above, it would take millions of years to guess your master password using generally-available password-cracking technology**. Your sensitive vault data, such as usernames and passwords, secure notes, attachments, and form-fill fields, remain safely encrypted based on LastPass' Zero Knowledge architecture. **There are no recommended actions that you need to take at this time**.
>
> **However, it is important to note that if your master password does not make use of the defaults above, then it would significantly reduce the number of attempts needed to guess it correctly. In this case, as an extra security measure, you should consider minimizing risk by changing passwords of websites you have stored**.

53. This statement revealed two remarkable facts. First, beginning in 2018 LastPass did not require legacy users to apply strong master passwords; and second, Toubba appears to be

[22] LastPass describes that the 2018 twelve-character master password requirement brought the number of "iterations" of the Password-Based Key Derivation Function up from 5,000 iterations to 100,000 iterations.

setting the stage to blame LastPass's legacy users if data thieves are able to crack pre-2018 master passwords.

54. In this notice, Toubba noted that LastPass had, at that point, only notified less than 3% of its business customers to recommend that they take action.

D. Plaintiff Suffered Harm as a Result of the Data Breaches

55. Plaintiff has been a customer of LastPass since January 17, 2011, using the service to protect all of his passwords—therefore also protecting all of his personally identifiable information, including the bank accounts, drivers' licenses, social security numbers, NEXUS IDs, and passports, as well as other financial information.

56. On December 22, 2022, Plaintiff received an email with the heading, "Update on Recent Security Incident," informing Plaintiff that an unauthorized third party gained access to the LastPass servers and subsequently accessed LastPass's store of personally identifiable user information.

57. Because website URL's are named as unencrypted user information compromised in the Data Breaches, data thieves possessing knowledge of the many user-specific web addresses for financial, bank, and brokers institutions will be able to prioritize Plaintiff's vault for decryption.

58. As a result of the Data Breaches, Plaintiff has needed to take multiple steps to protect himself against further data breaches.

59. Specifically, Plaintiff has, to date, spent approximately 120 hours changing every password once saved to the vault.

60. Plaintiff has also undertaken the process of closing every bank and brokerage account linked to his name, only to then reopen them with new account numbers. This required

coordinating with banks in Canada regarding the closing of the account and procurement of a new account card.

61. Plaintiff has also undertaken the process of canceling every credit card linked to his name.

62. These harms, and those suffered by the Class, were the direct result of LastPass's failure to secure users' personally identifiable information against and protect it during the August 2022 Data Breach and Second 2022 Data Breach.

E. Industry Backlash: Data Privacy and Security Experts Speak Out

63. Following LastPass's December revelation, a number of security experts spoke out against LastPass's handling of the data privacy and security failure and warning that LastPass was downplaying the risks and harms from the Data Breaches.

64. On December 26, 2022, security researcher Wladimir Palant published a blog post, "What's in a PR statement: LastPass breach explained."[23] In that post, Palant postured that the LastPass December 22 Statement was "full of omissions, half -truths and outright lies."

65. In his post, Palant raised three critical concerns relative to (1) the mischaracterization of the Data Breach sequence of events, (2) the consequences of data breaches involving IP addresses, and (3) the heightened risk for certain users depending on the profile and age of account.

66. First, Palant explained that LastPass's attempt to separate the initial August 2022 incident from the Data Breach is a mischaracterization of the sequence of events:

> LastPass is trying to present the August 2022 incident and the data leak now as two separate events. But using information gained in the initial access in order to access more assets is actually a typical technique used by threat actors. It is called lateral movement.

[23] *See* Wladimir Palant, What's in a PR statement: LastPass breach explained, Almost Secure (Dec. 26, 2022), https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/.

> So the more correct interpretation of events is: we do not have a new breach now, LastPass rather failed to contain the August 2022 breach. And because of that failure people's data is now gone. Yes, this interpretation is far less favorable of LastPass, which is why they likely try to avoid it.

67. Next, Palant explained the critical consequences of the fact that user IP addresses were stolen during the LastPass Data Breach:

> We learn [sic] that LastPass was storing your IP addresses. And since they don't state how many they were storing, we have to assume: all of them. And if you are an active LastPass user, that data should be good enough to create a complete movement profile. Which is now in the hands of an unknown threat actor.
>
> Of course, LastPass doesn't mention this implication, hoping that the less tech-savvy users won't realize.

68. A "movement profile" is a map of a user's geographic locations using the IP addresses saved to their device (or in the case of LastPass, their vault). A movement profile can be constructed by unauthorized third-party data thieves with access to a user's IP addresses by using the addresses to map the geographic location of the internet connection from a device. Geolocating using a user's IP addresses can provide a data thief with broad knowledge of a person's personal and private whereabouts on a daily basis.[24]

69. Finally, Palant points out that LastPass's post-2018 requirement of a twelve-character minimum for master passwords is likely not utilized by many users, therefore putting a large category of users at heightened risk for further cyber attacks due to the LastPass Data Breach:

> If you are a LastPass customer, chances are that you are completely unaware of this requirement. That's because LastPass didn't ask existing customers to change their master

[24] As an example of the data-privacy implications for the use of movement profiles and geolocation data, *see* Natasha Singer and Brian X. Chen, *In a Post-Roe World, the Future of Digital Privacy Looks Even Grimmer*, New York Times (Jul. 20, 2022) https://www.nytimes.com/2022/07/13/technology/personaltech/abortion-privacy-roe-surveillance.html. *See also* Sarah Emerson, *FTC Sues Geolocation Marketplace Over Abortion, Domestic Abuse Center Location Data*, Forbes (Aug. 29, 2022), https://www.forbes.com/sites/sarahemerson/2022/08/29/ftc-sues-geolocation-marketplace-over-abortion-domestic-abuse-center-location-data/?sh=2640d7461a35.

> password. I had my test account since 2018, and even today I can log in with my eight-character password without any warnings or prompts to change it.
>
> So LastPass required twelve characters for the past four years, but a large portion of their customer base likely still uses passwords not complying with this requirement. And LastPass will blame them should their data be decrypted as a result.

70. On December 27, 2022, security researcher Jeremi Gosney published a longform post on the platform Mastodon, stating that LastPass's claim of "zero knowledge" is a "bald-faced lie"[25]:

> They have about as much knowledge as a password manager can possibly get away with. Every time you login to a site, an event is generated and sent to LastPass for the sole purpose of tracking what sites you are logging into. You can disable telemetry, except disabling it doesn't do anything - it still phones home to LastPass every time you authenticate somewhere. Moreover, **nearly everything in your LastPass vault is unencrypted**. I think most people envision their vault as a sort of encrypted database where the entire file is protected, but no -- with LastPass, your vault is a plaintext file and only a few select fields are encrypted.

71. Gosney went on to explain LastPass's history of negligence in suffering seven major security breaches in the last 10 years:

> LastPass has suffered 7 major #security breaches (malicious actors active on the internal network) in the last 10 years. I don't know what the threshold of 'number of major breaches users should tolerate before they lose all faith in the service' is, but surely it's less than 7.

72. On December 28, 2022, an industry competitor of LastPass, 1Password, published a post on its own website titled, "Not in a million years: It can take far less to crack a LastPass password."[26] In that post, 1Password principal security architect Jeffrey Goldberg described LastPass's statement that it would take a million years to crack a LastPass master password as "highly misleading." Stating that the statistic was seemingly based off the post-2018 requirement that passwords be 12 characters and randomly generated, Goldberg explained that human-

---

[25] *See* Jeremi Gosney, @epixoip@infosec.exchange, Mastodon (Dec. 27, 2022), https://infosec.exchange/@epixoip/109585049354200263.

[26] *See* Jeffrey Goldberg, *Not in a million years: It can take far less to crack a LastPass password*, (Dec. 28, 2022), https://blog.1password.com/not-in-a-million-years/.

generated passwords come nowhere close to meeting that requirement, and that data thieves would be able to prioritize certain guesses based on how people build passwords they can actually remember.

V. CLASS ACTION ALLEGATIONS

73. Plaintiff brings these claims on behalf of the following Class:

> All individual persons whose PII was exposed, accessed, or otherwise compromised while in the possession of Defendants, or any of their subsidiaries and/or agents, as a result of the LastPass Data Breaches.

74. Plaintiff may alter the Class definitions to conform to developments in the case and discovery.

75. Excluded from the Class are Defendants, any entity in which Defendants have controlling interest, and Defendants' current or former officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

76. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), 23(b)(1), (b)(2), (b)(3), and (c)(4).

77. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The exact number of members of the Class is unknown to Plaintiff at this time, but LastPass states that over 33 million people and 100,000 businesses use LastPass. Ultimately, members of the Class will be easily identified through Defendants' records.

78. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) are satisfied. Common questions of fact and law exist for each cause of action and predominate over questions affecting individual members of the Class. Common questions for the Class include:

a) Whether Defendants engaged in the active misconduct of failing to adequately safeguard Plaintiff's and the Class Members' PII alleged herein;

b) Whether Defendants owed a duty to Plaintiff and the Class Members to safeguard and protect their PII;

c) Whether Defendants' computer systems and data security practices used to protect Plaintiff's and the Class Members' PII violated federal, state, and local laws, or Defendants' duties;

d) Whether Defendants breached their duties to Class Members to safeguard customer data;

e) What customer information was obtained by the unauthorized user as a result of the LastPass Data Breaches;

f) Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g) Whether Plaintiff and the Class Members suffered legally cognizable damages as a result of the LastPass Data Breaches;

h) Whether Defendants' failure to implement adequate data security practices proximately caused Plaintiff's and the Class Members' injuries;

i) Whether Plaintiff and the Class Members are entitled to restitution; and

j) Whether Plaintiff and the Class Members are entitled to declaratory and injunctive relief.

79. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members

sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them.

80. **Adequacy**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

81. **Predominance and Superiority**: All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class Members, and class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class Members. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides

the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

82. **Policies Generally Applicable to the Class**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants have acted or refused to act on grounds that apply generally to the Class, making final declaratory and/or injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply and affect Class Members uniformly, and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

83. **Particular Issues**: All requirements of Fed. R. Civ. P. 23(c)(4) are satisfied. Plaintiff's claims consist of particular issues that are common to all Class members and are capable of class-wide resolution that will significantly advance the litigation.

VI. CAUSES OF ACTION[27]

COUNT I
NEGLIGENCE

84. Plaintiff repeats and incorporates by reference, as though fully set forth herein, each and every allegation set forth in the paragraphs of this Complaint.

85. Defendants required Plaintiff and Class Members to submit PII in order to maintain a LastPass account and receive LastPass password and identity protection software and services.

86. Due to previous LastPass security issues, Defendants knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiff and Class Members.

[27] Plaintiff sent a demand letter to Defendants pursuant to Mass. G. L. Ch. 93A on the date of the filing of this complaint. Should good-faith negotiations resulting from the letter be unsuccessful, Plaintiff reserves the right to amend the complaint to add a claim under 93A.

87. Defendants owed duties of care to Plaintiff and Class Members whose PII had been entrusted with LastPass.

88. Defendants breached their duties to Plaintiff and Class Members by failing to provide adequate data privacy and security protocols to safeguard Plaintiff's and Class Members' PII.

89. Defendants acted with wanton disregard for the security of Plaintiff's and Class Members' PII. Defendants knew or should have known that Defendants had inadequate data privacy and security protocols to safeguard such information, and Defendants knew or should have known that data thieves were attempting to access the PII in password and identity protection software and services, such as LastPass.

90. A "special relationship" exists between Defendants and the Plaintiff and Class Members. LastPass entered into a "special relationship" with Plaintiff and Class Members because LastPass collected the PII of Plaintiff and Class Members and stored it in the LastPass Database—information that Plaintiff and the Class Members had been required to provide to LastPass in order to maintain a LastPass account.

91. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

92. The injury and harm suffered by Plaintiff and the Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties, and that Defendants' breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

93. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENT MISREPRESENTATION

94. Plaintiff repeats and incorporates by reference, as though fully set forth herein, each and every allegation set forth in the paragraphs of this Complaint.

95. Defendants negligently and recklessly misrepresented material facts, pertaining to the provision of password and identity protection software and services, to Plaintiff and Class Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft.

96. Further, once the initial August 2022 Breach was achieved by the unauthorized party, LastPass misrepresented material facts relative to the safety of user information to Plaintiff and Class Members on multiple occasions before finally exposing the full truth in the December 2022 Statement.

97. Because of a series of previous security incidents and knowledge of the initial August 2022 Breach, Defendants either knew or should have known that their representations were not true.

98. In reliance upon these misrepresentations, Plaintiff and Class Members obtained password and identity protection software and services from Defendants.

99. In further reliance upon these misrepresentations, Plaintiff and Class Members refrained from taking action to mitigate against any risk, based on guidance from LastPass prior to December 2022.

100. Had Plaintiff and Class Members, as reasonable persons, known of Defendants' inadequate data privacy and security protocols, or that Defendants were failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII, they would not have purchased password and identity protection software and services from Defendants, and would not have entrusted their PII to Defendants.

101. Further, had Plaintiff and Class Members, as reasonable persons, known of Defendants' failure to be transparent with Plaintiff and Class Members as to the fact that their PII was stolen in the LastPass Data Breaches, they would have acted sooner to mitigate against the risk of further breaches.

102. As a direct and proximate consequence of Defendants' negligent misrepresentations, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT III
BREACH OF EXPRESS CONTRACT

103. Plaintiff repeats and incorporates by reference, as though fully set forth herein, each and every allegation set forth in the paragraphs of this Complaint.

104. Plaintiff and Class Members entered into agreements with Defendants through (1), LastPass's Terms of Service for Personal Use, (2) LastPass's Terms of Service for Business Customers, and (3) LastPass's Terms of Service for Partner Sales. *See* ¶ 27.

105. Plaintiff and Class Members agreed to provide their PII to Defendants in exchange for Defendants agreeing to maintain and safeguard their PII.

106. Plaintiff and Class Members performed their material obligations under the contract of both (1) supplying Defendants their PII, and (2) paying Defendants for their password and identity protection software services.

107. Defendants breached their material obligations under the agreements with Plaintiff and Class Members by failing to maintain and protect the PII of Plaintiff and Class Members in accordance with the data privacy and security terms agreed upon by the parties.

108. As a direct and proximate result of Defendants' breach of these agreements, Plaintiff and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT

109. Plaintiff repeats and incorporates by reference, as though fully set forth herein, each and every allegation set forth in the paragraphs of this Complaint.

110. Plaintiff and Class Members entered into implied contracts with Defendants when they obtained password and identity protection software and services from Defendants, for which they were required to provide their PII. The exchange of PII provided by Plaintiff and Class Members to Defendants was also governed by and subject to LastPass's Terms of Service.

111. Defendants agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them in the event that their PII was breached, disclosed, or otherwise compromised.

112. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendants' data privacy and security protocols were compliant with relevant laws and regulations, consistent with industry standards, and in alignment with their own representations about LastPass's data privacy and security framework.

113. At all relevant times, Defendants had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and security protocol, including adequate prevention,

detection, and notification procedures, in order to safeguard the PII of Plaintiff and the Class Members, and to prevent the unauthorized access to and disclosure of this user data.

114. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Defendants of both (1) supplying Defendants their PII, and (2) paying Defendants for their password and identity protection software services.

115. Defendants breached their material obligations under the implied contracts with Plaintiff and Class Members by failing to maintain and protect the PII of Plaintiff and Class Members in accordance with the data privacy and security terms agreed upon by the parties.

116. As a direct and proximate result of Defendants' breaches of implied contracts, Plaintiff and the Class Members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

COUNT V
UNJUST ENRICHMENT

117. Plaintiff repeats and incorporates by reference, as though fully set forth herein, each and every allegation set forth in the paragraphs of this Complaint.

118. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of payments made for password and identity protection software and services.

119. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class Members' PII, as this was utilized by Defendants to facilitate payment to them.

120. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

121. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff the Class Members because Defendants failed to implement—or adequately implement—the data privacy and security practices and procedures for themselves that Plaintiff and the Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

122. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all proceeds obtained by Defendants through this inequitable and unlawful conduct.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class Members, respectfully requests the following relief:

A. Entry of an order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein;

B. Entry of an order appointing Plaintiff as representative of the Class;

C. Entry of an order appointing Plaintiff's counsel as co-lead counsel for the Class;

D. Entry of an order granting declaratory and injunctive relief prohibiting LastPass from engaging in the unlawful acts, omissions, and practices described herein;

E. Entry of judgment in favor of Plaintiff and each Class member for damages suffered as a result of the conduct alleged herein, including compensatory, statutory, and punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

F. Award of Plaintiff's reasonable litigation expenses and attorneys' fees to the extent allowed by law; and

G. Grant of such other and further legal and equitable relief as the Court deems just and equitable.

VIII. JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 18, 2023

Respectfully submitted,

/s/ Nathaniel L. Orenstein

BERMAN TABACCO
PATRICK T. EGAN (BBO #637477)
NATHANIEL L. ORENSTEIN (BBO #664513)
CHRISTINA L. GREGG (BBO #709220)
One Liberty Square
Boston, Massachusetts 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
norenstein@bermantabacco.com
cgregg@bermantabacco.com

BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr.
Albert Y. Chang
7817 Ivanhoe Ave., Suite 102
La Jolla, CA 92037
(858) 914-2001 telephone
(858) 914-2002 facsimile
fbottini@bottinilaw.com
achang@bottinilaw.com